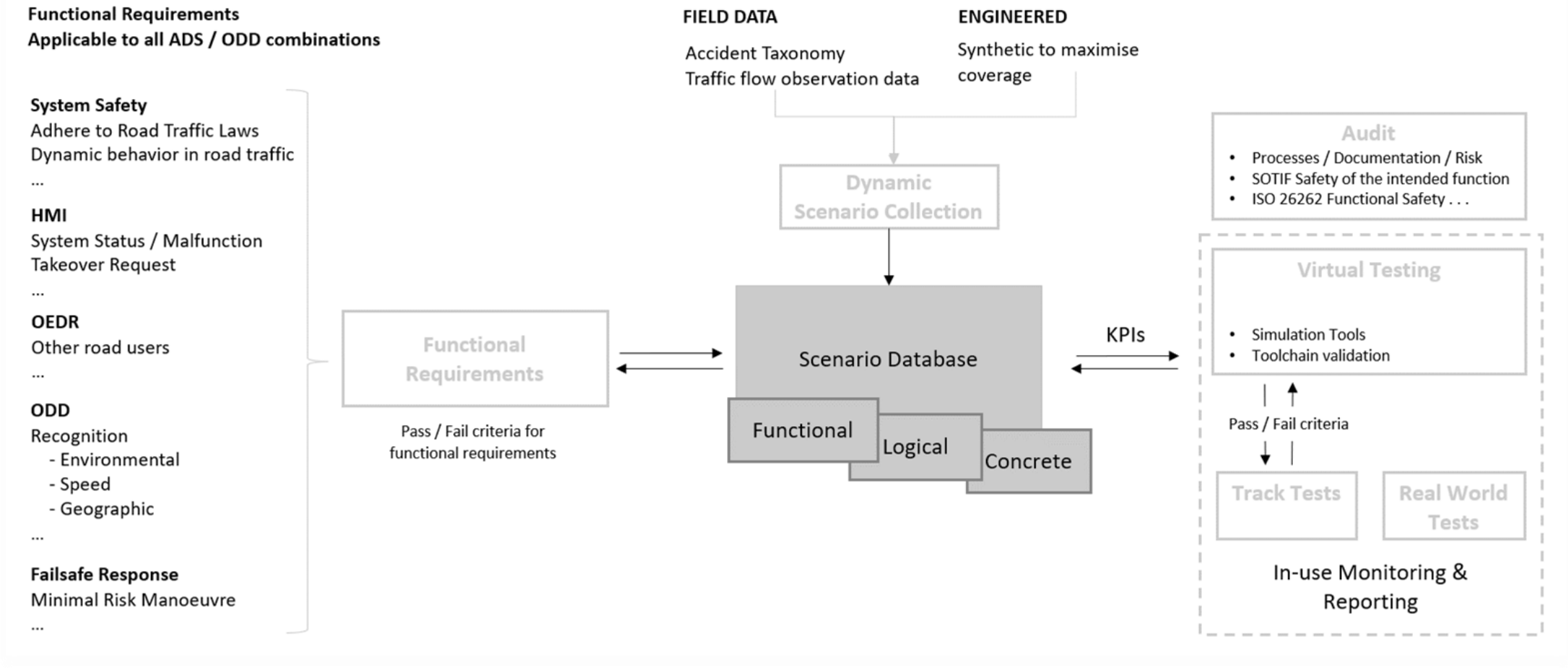
Automated Vehicles Certification

An Operational Design Domain (ODD) Framework

Matteo Oldoni | AI & Autonomous Driving Standards | NVIDIA

UNECE Regulatory Landscape



Operational Design Domain (ODD) Approach

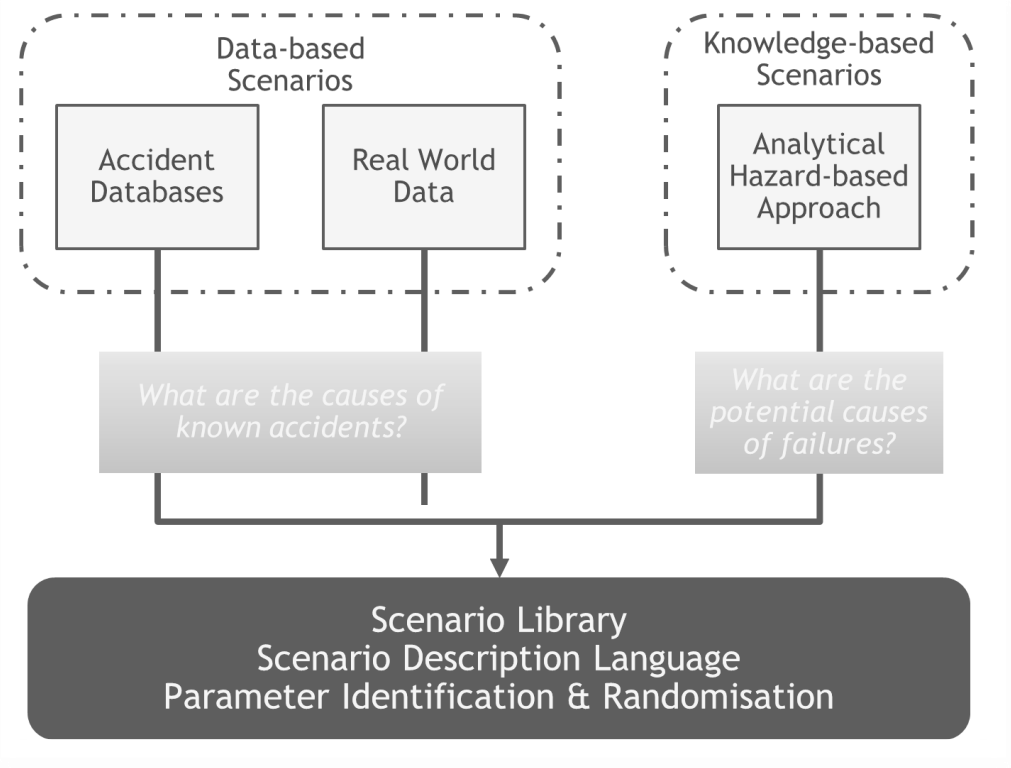
- Industry proposed approach aims to:
  - Map applicable Functional Requirements based on the Manufacturer ODD description
  - Generate scenario to assess the AV performance against relevant requirements
  - Derive measurable and verifiable criteria, assumptions and KPIs for scenario testing
- The approach does not focus on prescriptive criteria, however concentrate on how to implement existing tools / best practices well-known by OEMs
- What are the fundamentals of the ODD-based framework approach …

Scenario and ODD

- Scenarios are real-world traffic situations that ‘exercise and challenge’ the capabilities of an AV to operate safely
- Different types of scenarios can be used to assess the AV capabilities:
  - Nominal Scenarios – reasonably foreseeable situations for a given domain
  - Critical Scenarios – traffic scenarios edge-cases, or scenes engineered to spot functional insufficiencies
  - Failure Scenarios – system or sub-system E/E failures
- Operational Design Domain (ODD) refers to the AV operating environment (i.e. environmental conditions, scenery and dynamic elements, …)
- A scenario-based approach for certification requires an understanding of what scenario are applicable given the specific ODD

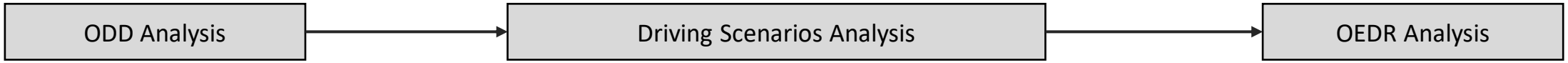
Scenario Generation

- What is the source of scenario?
  - Data-based (Nominal and Critical Scenario)
  - Knowledge-based (Critical and Failure Scenario)



Nominal Scenario

- Nominal scenarios and requirements can be derived from the ODD and the expected behaviour competency (analysis of Highway code and AV functional requirements)
  - The baseline ODDs is used to identify objects and events that could be encountered
  - Based on the objects and events identified it is possible to map the appropriate AV response
- Test parameters and assumptions are based on real-world data (e.g., real driving behaviour)
- The AV is expected to avoid a collision in these “nominal situations”



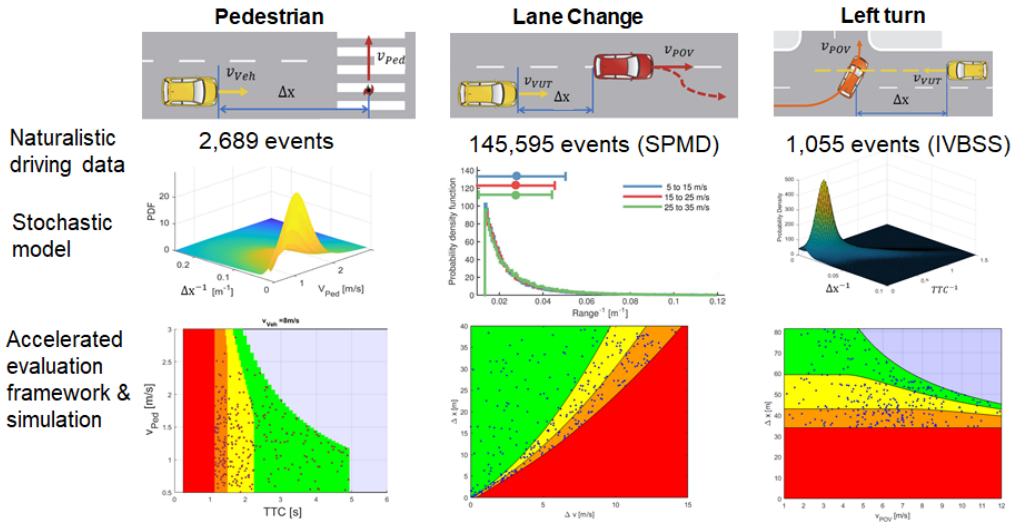
Perform analysis to identify the characteristics of the ODD

Perform driving scenario analysis
- Expected hazards
- Unspecified events
- Key infrastructure elements

Perform analysis to identify OEDR behaviors and corresponding responses.

Critical Scenario

- Derived from Nominal Scenario by applying tight assumptions (e.g., higher decel profile, cut-in…)
- Engineered based on the application of formal techniques (e.g., STPA, FMEA, FTA, …)
- These scenario aim to explore the envelope of AV performance (preventability vs unpreventability)
- The AV is not expected to avoid a collision in all possible situations, but performance are compared to safety models

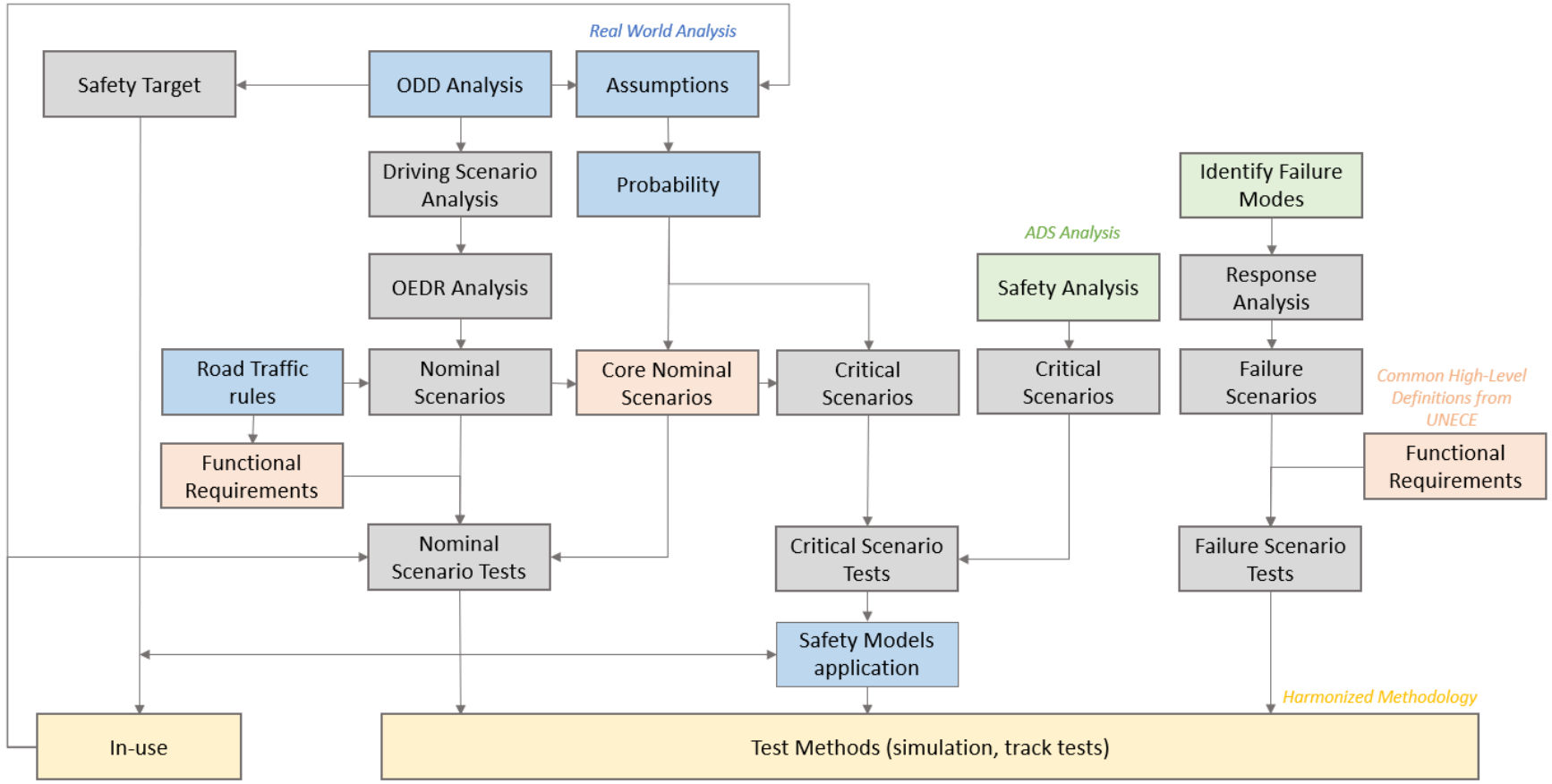


Mcity - Data collection, model fitting and test case generations

Failure Scenario

- Failure scenarios are engineered (e.g., FMEA, STPA, …)
  - Identify potential failures (e.g., sensing and comms, perception, navigation and control, …)
  - Identify potential causes and effects of those failure modes
  - Prioritize the failure modes based upon risk
  - Identify an appropriate corrective action or mitigation strategy
- After completing the FMEA for the AV architecture, the various failure modes and effects can be summarized and mapped to the relevant tactical maneuver and OEDR behaviors
- These scenario aim to assess the AV ability to detect and respond to system malfunctions
- Functional requirements are defined by Regulators

ODD Framework - Process Flowchart

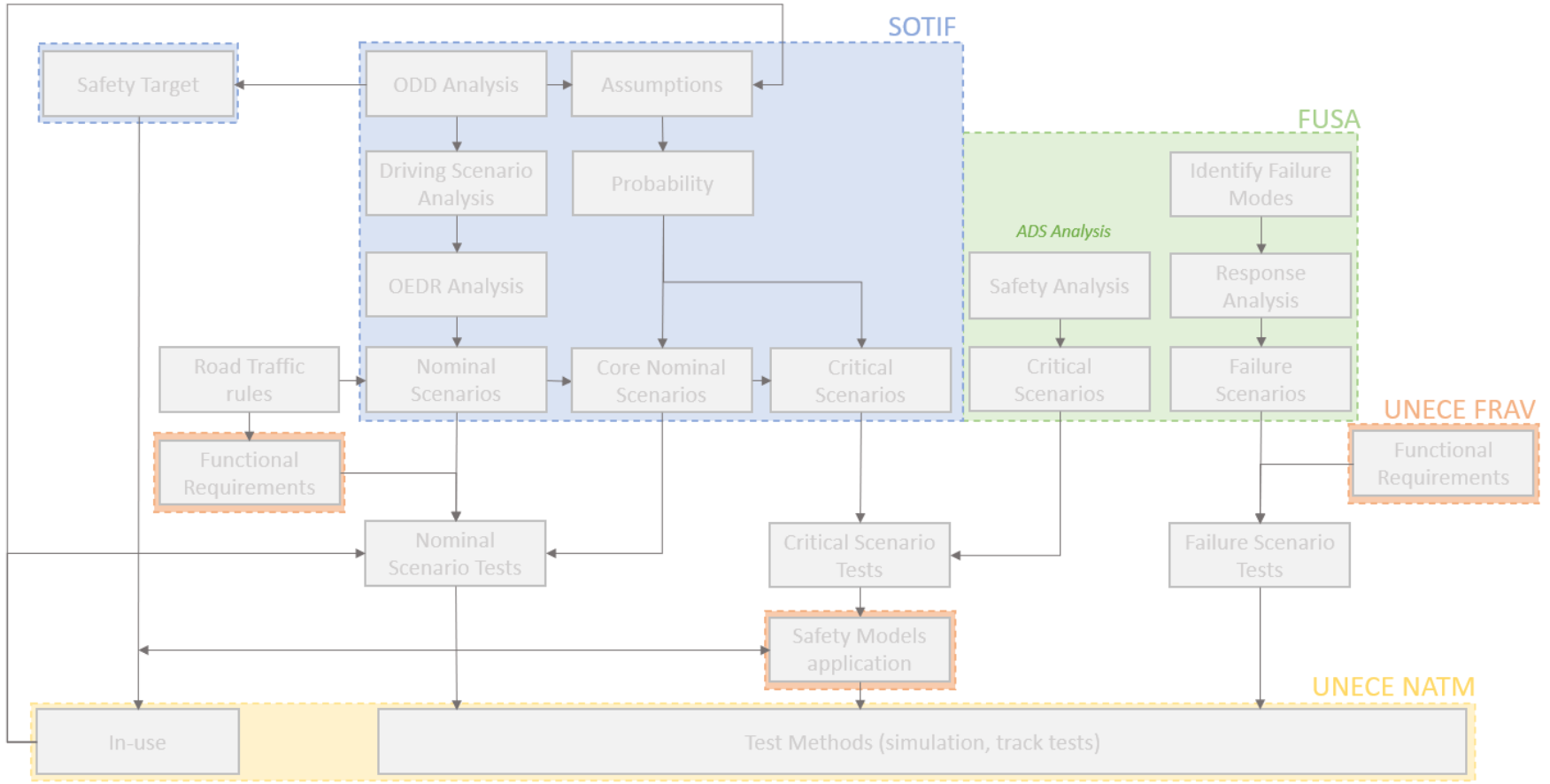


Summary

- The AV certification consists of a scenario-based assessment
- The manufacturer ODD description will support determination of applicable requirements and scenario generation
- The approach concentrate on how to implement existing tools without prescribing one
  - In Nominal scenarios the AV is expected to avoid collisions
  - In Critical scenario, the performance threshold is compared to safety models
  - In Failure scenario the AV is expected to detect and respond to system failures according to applicable UN requirements
- Measurable criteria / use of specific tools may be harmonised with more real-world experience

Thank you for your attention!

ODD Framework – Use of Existing Tools



Example of Nominal Scenario

ODD (Dynamic) Element		Driving Behaviour	Traffic Rule	Functional Requirement	Behaviour Competency	Assumption	Test Scenario	Pass/Fail Criteria
Bicycle		Riding in lane (Frontal)	Drivers will also need to use a minimum passing distance for bicycles of 1.5m in urban areas, and 2m out of town	The ADS should adapt its behaviour in line with safety risks	ADS should ensure relative velocity during passing manoeuver doesn't exceed [30]km/h	bicycle Vlong 4.3 [SD 0.57] (Avg) m/s	The ADS shall travel between [30-50]km/h on the centre line of the road. A cyclist shall travel in the same direction as the ADS between [10-20]km/h, [0.2-1]m away from the lane edge. Test scenarios that require lane crossing shall be conducted with/without oncoming traffic.	The relative speed between the cyclist and the ADS shall not exceed 30km/h
				The ADS should comply with road traffic rules	Shift in lane to pass by cyclist with 1.5m lateral distance			The passing distance between the cyclist and ADS is not less than 1.5m
				The ADS behaviour should not disrupt the flow of traffic	The ADS may cross the center lane marking to ensure the safe passing distance is not violated			The ADS may cross the center lane marking to ensure the safe passing distance is not violated
				The ADS should interact safely with other road users	The ADS shall activate the turn signal if the center lane marking is crossed			The ADS activates the turn signal if the center lane marking is crossed
Speed Sign		Lower speed limit (Frontal)	You must not exceed 70 mph (112 km/h), or the maximum speed limit permitted for your vehicle. If a lower speed limit is in force, either permanently or temporarily, at road works for example, you must not exceed the lower limit.	The ADS should comply with road traffic rules	The ADS should ensure the absolute velocity of the ego vehicle does not exceed the designated speed limit when passing the sign			The ADS shall not exceed the speed limit indicated by the traffic sign.
Speed Sign		Higher speed limit (Frontal)	You must not exceed 70 mph (112 km/h), or the maximum speed limit permitted for your vehicle. If a lower speed limit is in force, either permanently or temporarily, at road works for example, you must not exceed the lower limit.	The ADS should comply with road traffic rules	The ADS should ensure the absolute velocity of the ego vehicle does not exceed the designated speed limit when passing the sign			The ADS shall not exceed the speed limit indicated by the traffic sign.
				The ADS behaviour should not disrupt the flow of traffic	The ADS should attempt to travel at the speed limit unless it is not aligned with safety risks			
				The ADS should adapt its behaviour in line with safety risks	The ADS should travel at a speed that ensure that the entire length of the stopping distance is visible			
Heavy rain			In wet weather you should keep well back from the vehicle in front. This will increase your ability to see and plan ahead	The ADS should adapt its behaviour in line with safety risks	The ADS should increase the minimum headway behind the lead vehicle			
				The ADS should adapt its behaviour in line with safety risks	The ADS should travel at a speed that ensure that the entire length of the stopping distance is visible			

Example of Critical Scenario

Losses	Hazards	ODD	Control Structure	Control Actions	Unsafe Control Action	Loss Scenario	Casual Factors	Assumption	Test Behaviour	Test Scenario	Pass/Fail Criteria
Collision with objects outside the vehicle	Vehicle does not maintain safe distance from lead motor vehicle	Urban Environment Day and Night All weather conditions	Level 4 (no Driver) Sensors: LIDAR, RADAR, Camera Actuation: Brake, Accelerator, Steering no V2X	Request braking command	Braking demand is not requested	Object in vehicle trajectory is not detected	undetected / misclassified objects obscured object Incorrect sensor fusion results	lead Vehicle deceleration 7.0 [SD 2.3] (Dry) 4.4 [SD 1.0] (Wet) (Max Avg) m/s2	ADS is following behind a lead vehicle. Headway between the two vehicles is set by the ADS. Lead vehicle decelerates at the max assumed rates depending on the weather conditions	Lead vehicle decelerates to turn [Right / Left] or travel straight on at a [mini / large] roundabout	The ADS avoids a collision with the lead vehicle
						Object is not considered to be in the vehicle trajectory	Localisation issues leading to incorrect positioning of ego vehicle or object			Lead vehicle decelerates whilst shifting in lane to avoid [static object / other road user]	The ADS avoids a collision with the lead vehicle
					Braking demand is requested too late after conflict is unavoidable	Object in vehicle trajectory is not detected	undetected / misclassified objects obscured object Incorrect sensor fusion results			Lead vehicle decelerates whilst travelling on straight road with thick foliage and overhanging trees	The ADS avoids a collision with the lead vehicle
						Object is not considered to be in the vehicle trajectory	Localisation issues leading to incorrect positioning of ego vehicle or object				

Example of Failure Scenario

Failure Type	Failure Mode	Potential Cause	Response	Functional Requirement	Assumption	Test Scenario	Pass/Fail Criteria
Perception	Fail to identify ODD boundary	Failure to detect ODD attribute e.g. Heavy Rain / Fog	Safely stop in lane of travel	The ADS shall be able to detect the ODD and predict when the ADS is about to leave the ODD	N/A	The ADS shall operate upto and beyond the predfined ODD. ODD characteristic to consider include geographical area and weather conditions	The ADS detects the ODD conditions are not met and issues a minimal risk manoeuver.
				When the system detects that it is difficult to continue in the automated driving mode, it shall be able to transfer to a minimal risk condition (with or without take over request) through a minimal risk manoeuvre.			The minimum risk manoeuver should not cause the vehicle to decelerate greater than 4m/s2
				Other road users and occupants shall be informed that the vehicle is performing a minimum risk manoeuvre in accordance with applicable traffic rules (e.g. hazard lights, brake lights, turning indicators)			The ADS should activate the hazard lights through out the minimal risk manoeuver.
				The Minimum Risk Manoeuvre (MRM) shall comply with traffic rules.			The ADS shall use the turn indicator when changing lanes.

Useful Links

- ADS Safety Requirements, UNECE
- A Framework for Automated Driving System Testable Cases and Scenarios, NHTSA
- Mapping Requirements for Nominal Lane Keeping Scenario, OICA/CLEPA, UNECE
- New Assessment and Test Methods (NATM) for AVs, UNECE
- Safety Models for AVs, UNECE
- A Testing Method for Highly Automated Vehicles, Mcity